#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: KILKKILÄ

Serial No. TO BE ASSIGNED

Corresponding to PCT/FI00/00699, filed August 17, 2000

Filed: January 24, 2002 Docket No.: 602.361USW1

Title: METHOD AND SYSTEM FOR IDENTIFICATION IN A TELECOMMUNICATION SYSTEM

CERTIFICATE UNDER 37 C.F.R. 1.10:
'Express Mail' mailing number: EV017368386US
Date of Deposit: 1/24/02
The undersigned hereby certifies that this Transmittal Letter and the paper or fee, as described herein, are being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

By: Lee Thao
Lee Thao

SUBMISSION OF PRIORITY DOCUMENT

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is a certified copy of Finnish application, Serial Number 19991812, filed 08/25/99, the priority of which is claimed under 35 U.S.C. §119.

Respectfully submitted,

Altera Law Group, LLC
6500 City West Parkway, Suite 100
Minneapolis, Minnesota 55344-7701
952-253-4100

Date: 1-24-02

By: _____
Michael B. Lasky
Reg. No. 29,555

MBL/mar/ems

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 27.11.2001

E T U O I K E U S T O D I S T U S
P R I O R I T Y D O C U M E N T

Hakija Applicant	**Nokia Telecommunications Oy** **Helsinki**
Patenttihakemus nro Patent application no	**19991812 (pat.106899)**
Tekemispäivä Filing date	**25.08.1999**
Kansainvälinen luokka International class	**H04L 9/32**

Keksinnön nimitys
Title of invention

"Menetelmä ja järjestelmä tunnistamiseen tietoliikennejärjestelmässä"

Hakijan nimi on hakemusdiaariin **12.12.1999** tehdyn nimenmuutoksen jälkeen **Nokia Networks Oy**.

The application has according to an entry made in the register of patent applications on **12.12.1999** with the name changed into **Nokia Networks Oy**.

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kalla
Tutkimussihteeri

CERTIFIED COPY OF
PRIORITY DOCUMENT

Maksu 300,- mk
Fee 300,- FIM

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1782/1995 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1782/1995 concerning the chargeable services of the National Board of Patents and Registration of Finland.

MENETELMÄ JA JÄRJESTELMÄ TUNNISTAMISEEN TIETOLIIKENNEJÄRJESTELMÄSSÄ

KEKSINNÖN ALA

Esillä oleva keksintö liittyy tietoliikennejärjestelmiin. Erityisesti keksinnön kohteena on menetelmä ja järjestelmä käyttäjän tunnistamiseksi ja osapuolten varmistamiseksi tietoliikennejärjestelmässä.

KEKSINNÖN TAUSTA

Tietoliikenneverkko, esimerkiksi puhelinverkko koostuu useista erillisistä komponenteista, jotka on kytketty toisiinsa siirtojohdoilla. Eräs tällainen komponentti on puhelinkeskus, joka on esimerkiksi hakijan valmistama DX 200. Puhelinverkkoa hallitaan ja huolletaan käytönohjausverkolla (O&M-network, Operation and Maintenance), joka voidaan toteuttaa esimerkiksi X.25-pakettiverkon palveluihin pohjautuen. Käytönohjausverkko muodostetaan kytkemällä puhelinkeskukset ja muut ohjauksen alaiset verkkokomponentit siihen. Muita ohjauksen alaisia verkkokomponentteja ovat esimerkiksi transkooderi (TC, TransCoder), tukiasema (BTS, Base Transceiver Station) ja tukiasemaohjain (BSC, Base Station Controller).

Käytönohjausverkkoon liittyneenä olevista puhelinverkkoelementeistä voidaan muodostaa etäistuntoja muihin käytönohjausverkkoon yhdistettyihin puhelinkeskuksiin tai verkkoelementteihin. Muodostettaessa etäistuntoa lähdejärjestelmästä kohdejärjestelmään kohdejärjestelmälle lähetetään käyttäjäkohtaisia tietoja tunnistusta varten. Lähde- ja kohdejärjestelmät ovat esimerkiksi puhelinkeskuksia. Käyttäjäkohtaisia tietoja ovat esimerkiksi käyttäjätunnus ja siihen liittyvä salasana. Usein lähetettävä salasana salataan sopivalla salausalgoritmilla väärinkäytösten estämiseksi. Salausalgoritmi on esimerkiksi ns. yksisuuntainen algoritmi. Tämä tarkoittaa sitä, että salauksen

lopputuloksesta ei ole mahdollista päätellä tai muodostaa alkuperäistä syötettä. Kaksisuuntainen algoritmi tarkoittaa sitä, että salauksen lopputulos on mahdollista purkaa selväkieliseksi. Yleensä purku tapahtuu samalla algoritmilla, jolla itse salaus on tehty. Purkamisessa voidaan käyttää joko samaa tai eri salausavainta kuin salattaessa. Ensiksi mainittua tapaa kutsutaan symmetriseksi ja jälkimmäistä epäsymmetriseksi salaukseksi.

Salausalgoritmien käyttö parantaa turvallisuutta, mutta ei poista kaikkia turvallisuuteen liittyviä ongelmia. Joissain tapauksissa on mahdollista, että ulkopuolinen taho monitoroi linjaa, jossa kulkee etäistuntoon liittyviä sanomia. Tällöin ulkopuolisella taholla saattaa olla mahdollisuus kaapata istuntoon liittyvät aloitussanomat ja simuloida etäistunnon aloittaminen käyttäen salattua salasanaa ja asianmukaista käyttäjätunnusta.

Edellä mainituissa kohdissa on ongelmana tunnistaa käyttäjä varmuudella. Edelleen ongelmana on se, että etäistuntoon liittyvät lähde- ja kohdejärjestelmä eivät voi olla varmoja toistensa alkuperästä.

Keksinnön tarkoituksena on poistaa edellä mainitut epäkohdat tai ainakin merkittävästi lieventää niitä. Erityisesti keksinnön tarkoituksena on tuoda esiin uudentyyppinen menetelmä, joka mahdollistaa käyttäjän tunnistamisen varmuudella kohdejärjestelmässä ja etäistuntoon liittyvien järjestelmien alkuperäisyyden varmistamisen.

Esillä olevan keksinnön tunnusomaisten seikkojen osalta viitataan patenttivaatimuksiin.

KEKSINNÖN YHTEENVETO

Keksinnön mukainen menetelmä koskee käyttäjän tunnistamista ja osapuolten varmistamista tietoliikennejärjestelmässä. Keksinnön mukainen tietoliikennejär-

jestelmä käsittää tietoliikenneverkon ja siihen yhdistetyt lähde- ja kohdejärjestelmät.

Menetelmässä tallennetaan lähde- ja kohdejärjestelmään käyttäjätunnukset ja niihin liittyvät salasanat. Edelleen kirjaudutaan lähdejärjestelmään syöttämällä käyttäjätunnus ja sitä vastaava salasana. Käyttäjä tunnistetaan lähdejärjestelmässä käyttäjätunnuksen ja salasanan perusteella. Edelleen muodostetaan etäistunto lähdejärjestelmästä kohdejärjestelmään.

Keksinnön mukaisesti muodostetaan lähde- ja kohdejärjestelmään identtiset indeksoidut salausavaimet. Salausavaimet voidaan muodostaa tietyllä ennalta määritellyllä salausalgoritmilla esimerkiksi indeksin perusteella. Lähde- ja kohdejärjestelmä voivat sisältää myös erityisen salausavainlistan tai -tiedoston, joka sisältää useita salausavaimia. Istunnon muodostamisen ensimmäisessä vaiheessa salataan käyttäjätunnukseen liittyvä salasana lähdejärjestelmässä ensimmäisen indeksin osoittamalla salausavaimella ja lähetetään salatut tiedot sekä ensimmäinen indeksi ja käyttäjätunnus kohdejärjestelmälle. Indeksiä ja käyttäjätunnusta ei siis välttämättä lähetetä järjestelmien välillä salatussa muodossa. Indeksi ja käyttäjätunnus voidaan lähettää suojaamattomina siksi, että niiden julkisuus ei vähennä järjestelmän turvallisuutta, koska indeksin perusteella ei voida selvittää sitä vastaavaa salausavainta. Indeksi ja käyttäjätunnus voidaan lähettää myös salattuna, jolloin ne salataan käyttämällä esimerkiksi kaksisuuntaista salausalgoritmia. Lähdejärjestelmä voi lähettää kohdejärjestelmälle myös erillisen tunnistetiedon, joka salataan ja lähetetään kohdejärjestelmälle samanaikaisesti käyttäjätietojen kanssa edellä kuvatun menettelyn mukaisesti. Tunnistetieto voidaan välittää lähde- ja kohdejärjestelmän välillä myös itsenäisesti, erillään käyttäjätiedoista muuna ajankohtana.

Ensimmäinen indeksi tarkoittaa edullisesti lukua tai kohtaa, joka osoittaa johonkin tiettyyn salausavaimeen. Indeksi voidaan valita satunnaisesti tai se voidaan muodostaa jonkin ennalta määritellyn algoritmin pohjalta. Tämä algoritmi voi olla salainen ja ainoastaan lähde- ja kohdejärjestelmän tiedossa. Tunnistetieto tarkoittaa esimerkiksi aikatietoa ja/tai lähdejärjestelmän yksilöivää tietoa. Aikatieto saadaan esimerkiksi järjestelmän kellosta ja lähdejärjestelmän yksilöivä tunniste esimerkiksi konfigurointitiedostoista.

Kohdejärjestelmä vastaanottaa lähdejärjestelmän lähettämän sanoman, johon kuuluu edullisesti salattu salasana, käyttäjätunnus, indeksi ja mahdollisesti tunnistetieto. Kohdejärjestelmässä etsitään kyseiseen käyttäjätunnukseen liittyvä salasana salasanalistasta ja salataan käyttäjätunnukseen liittyvä salasana indeksin osoittamalla salausavaimella. Käyttäjätunnukseen liittyvä salasana on tallennettuna käyttäjätietoihin kohdejärjestelmässä. Kohdejärjestelmä vertaa vastaanotettua salasanaa ja juuri salaamaansa salasanaa. Etäistunnon muodostaminen voidaan estää, jos vertailtavat salatut salasanat eivät ole yhteneväisiä.

Tämän jälkeen toisessa vaiheessa kohdejärjestelmä salaa lähdejärjestelmältä vastaanotetun käyttäjätunnukseen liittyvän salasanan ja mahdollisesti tunnistetiedon toisen indeksin osoittamalla salausavaimella. Salatut tiedot sekä toinen indeksi lähetetään takaisin lähdejärjestelmälle, jossa kohdejärjestelmälle alussa lähetetty salattu salasana salataan uudestaan kohdejärjestelmältä juuri vastaanotetun toisen indeksin osoittamalla salausavaimella. Saatua tulosta verrataan kohdejärjestelmältä vastaanotettuun salattuun salasanaan. Etäistunnon muodostaminen voidaan estää, jos vertailtavat salatut salasanat eivät ole yhteneväisiä.

Jos käytetään tunnistetietoa lähde- ja kohdejärjestelmän välillä, kohdejärjestelmälle alussa lähetetty ensimmäisen indeksin osoittamalla salausavaimella salattu tunnistetieto salataan uudestaan lähdejärjestelmässä kohdejärjestelmältä vastaanotetun toisen indeksin osoittamalla salausavaimella. Lähdejärjestelmässä verrataan juuri salattua tunnistetietoa kohdejärjestelmältä vastaanotettuun salattuun tunnistetietoon. Etäistunnon muodostaminen voidaan estää, jos vertailtavat salatut tunnistetiedot eivät ole yhteneväisiä. Tunnistetiedon käytön avulla lähdejärjestelmä voi varmistua kohdejärjestelmästä. Lähdejärjestelmähän voi lähettää alussa salatun tunnistetiedon kohdejärjestelmälle. Jos kohdejärjestelmä on oikea, se lähettää saman tunnistetiedon lähdejärjestelmälle uudella salausavaimella salattuna. Koska lähdejärjestelmä saa kohdejärjestelmältä samalla toisen indeksin, joka osoittaa tiettyyn salausavaimeen, lähdejärjestelmä pystyy vertailutoimenpiteellä vahvistamaan tunnistetietojen yhteneväisyyden ja näin samalla varmistuu kohdejärjestelmästä. Tunnistetietoa ei siis tarvitse välttämättä välittää samanaikaisesti käyttäjätietojen kanssa, vaan se voidaan välittää myös erikseen sopivana ajankohtana.

Jos edellä mainittujen vertailujen tulokset ovat yhteneväisiä, etäistunto voidaan muodostaa.

Eräässä keksinnön sovelluksessa käytetään lähde- ja kohdejärjestelmässä tiedon salaukseen yksisuuntaista salausalgoritmia. Esimerkkejä tällaisista algoritmeista ovat MD5 (MD5, Message Digest 5) ja SHA (SHA, Secure Hash Algorithm).

Eräässä keksinnön sovelluksessa tietoliikennejärjestelmä on puhelinkeskusjärjestelmä.

Eräässä keksinnön sovelluksessa lähde- ja/tai kohdejärjestelmä ovat puhelinkeskuksia.

Eräässä keksinnön sovelluksessa tietoliikenneverkko on käytönohjausverkko.

Esillä olevan keksinnön mukainen järjestelmä käsittää välineet identtisten indeksoitujen salausavainten muodostamiseksi lähdejärjestelmään ja kohdejärjestelmään, välineet tietojen salaamiseksi lähde- ja kohdejärjestelmässä indeksin osoittamalla salausavaimella ja välineet tietojen lähettämiseksi lähde- ja kohdejärjestelmän välillä. Edelleen järjestelmä käsittää välineet vertailun tekemiseksi lähde- ja kohdejärjestelmässä ja välineet etäistunnon muodostuksen hyväksymiseksi.

Eräässä keksinnön sovelluksessa järjestelmä käsittää välineet etäistunnon muodostamisen estämiseksi. Eräässä toisessa sovelluksessa järjestelmä käsittää välineet tunnistetiedon muodostamiseksi ja aikatiedon ja/tai lähdejärjestelmän yksilöivän tiedon liittämiseksi tunnistetietoon.

Eräässä keksinnön sovelluksessa järjestelmä käsittää salausavainlistan salausavainten tallentamista varten.

Eräässä keksinnön sovelluksessa järjestelmä käsittää välineet indeksin muodostamiseksi satunnaisesti tai jonkin ennalta määritellyn algoritmin pohjalta.

Keksinnön etuna on se, että itse salausavaimia ei missään vaiheessa lähetetä järjestelmien välillä. Keksinnön ansiosta käyttäjä tunnistetaan kohdejärjestelmässä varmuudella ja samalla varmistutaan etäistunnon käsittävien järjestelmien alkuperästä.

KUVALUETTELO

Seuraavassa keksintöä selostetaan yksityiskohtaisesti sovellusesimerkkien avulla, jossa

kuva 1 esittää erästä edullista järjestelmää, jossa keksinnön mukainen menetelmä voidaan toteuttaa,

kuva 2 esittää erästä keksinnön mukaista ohjelmalohkoa, joka on yhdistetty puhelinkeskukseen, ja

kuva 3 esittää erästä edullista keksinnön mukaista vuokaavioesimerkkiä.

KEKSINNÖN YKSITYISKOHTAINEN SELOSTUS

Kuvan 1 mukaiseen järjestelmään kuuluu käytönohjausverkko OM, lähdejärjestelmä LE1, kohdejärjestelmä LE2 ja työasema TE. Lähdejärjestelmä LE1 ja kohdejärjestelmä LE2 ovat edullisesti puhelinkeskuksia. Puhelinkeskus on esimerkiksi hakijan valmistama DX 200. Työasema TE on yhdistetty lähdejärjestelmään LE1 ja työasemalla on mahdollista muodostaa etäistuntoja lähdejärjestelmän kautta kohdejärjestelmään LE2. Etäistunto muodostetaan käytönohjausverkon OM kautta. Työasema voi olla tavallinen PC-tietokone tai vastaava, johon kuuluu näyttö ja näppäimistö, joiden avulla käyttäjä voi interaktiivisesti välittää tietoa käytönohjausverkon OM kanssa.

Lisäksi kuhunkin keskukseen kuuluu ohjelmalohko PB (PB, Program Block), joka on DX 200 -keskuksessa tietty ohjelmiston ja oheislaitteiden muodostama kokonaisuus, jonka avulla operaattori voi suorittaa käytönohjausfunktioita käytönohjausverkossa OM. Käytännössä ohjelmalohko PB on käyttäjän ja koneen tai puhelinkeskuksen välinen liitäntä, jolla käyttäjä voi liittyä ja antaa komentoja järjestelmään. Tätä lohkoa kuvataan yksityiskohtaisemmin kuvan 2 yhteydessä. Kuvassa 1 esitetty järjestelmä on eräs edullinen esimerkki mahdollisesta järjestelmästä, jossa keksinnön mukainen menetelmä voidaan toteuttaa.

Kuvassa 2 esitetään tarkemmin ohjelmalohkon PB rakennetta ja toimintaa. Ohjelmalohkoon voi kuulua muitakin komponentteja kuin mitä kuvassa 2 on esitetty. Ohjelmalohkoon kuuluu käytönohjauslohko MMSSEB (Man Machine Interface System Service Block). Käytönohjauslohko on yhdistetty syöttö- ja tulostuspalvelulohkoon 20, joka tarjoaa muille käytönohjauslohkoille syöttö- ja tulostusjärjestelmä-

palveluja. Lohkolla 20 kytketään käytönohjauslohko ulkoisiin lisälaitteisiin, kuten näyttöön, näppäimistöön, tulostimeen ja tallennuslaitteeseen. Käytönohjauslohko on lisäksi yhdistetty tietoliikennelohkoon 23 ja turvapalvelulohkoon 25.

Lisäksi kuvassa 2 esitettyyn käytönohjauslohkoon MMSSEB kuuluu kohteenvalintalohko 21, jolla valitaan se järjestelmä, johon käyttäjä haluaa muodostaa istunnon. Käytännössä järjestelmä voi olla paikallinen järjestelmä eli lähdejärjestelmä, johon käyttäjän työasema on kytketty tai se voi olla jokin etäjärjestelmä eli kohdejärjestelmä, johon yhteys muodostetaan käytönohjausverkon kautta.

Käyttäjän istuntoa ohjataan istunnonohjauslohkolla 22, joka on yhteydessä kohteenvalintalohkoon 21, tietoliikennelohkoon 23 ja käyttäjänhallintalohkoon 24. Istunnonohjauslohko ohjaa istuntoa käyttäjän antamien komentojen perusteella. Käyttäjänhallintalohko tarjoaa muun muassa käyttäjäntunnistus- ja valtuustarkastuspalveluita. Tietoliikennelohkolla käytönohjauslohko MMSSEB muodostaa etäyhteydet muissa esimerkiksi puhelinkeskuksissa oleviin käytönohjauslohkoihin kohteenvalintalohkon ohjauksen mukaisesti. Käytännössä tietoliikennelohko toimii rajapintana ja puskurina lähde- ja kohdejärjestelmän välillä.

Tietoliikennelohko 23 käsittää ohjelmalohkon 3, jonka avulla lähetetään tietoja eri ohjelmalohkojen tai järjestelmien välillä. Istunnonohjauslohko 22 käsittää välineet 7 tunnistetiedon muodostamiseksi ja aikatiedon liittämiseksi tunnistetietoon. Välineillä 7 tarkoitetaan esimerkiksi ohjelmalohkoa, joka kykenee selvittämään aikatiedon ja liittämän sen osaksi tunnistetietoa. Tunnistetietoa voidaan käyttää apuna tiedonsiirron välisten osapuolten tunnistamisessa. Aikatieto selvitetään esimerkiksi käytönohjauslohkon MMSSEB käsittävän isomman järjestelmän kellosta. Is-

tunnonohjauslohko käsittää lisäksi ohjelmalohkon 9, jolla muodostetaan indeksi satunnaisesti tai jonkin ennalta määritellyn algoritmin pohjalta. Indeksi tarkoittaa esimerkiksi numeroarvoa, joka viittaa tiettyyn salausavaimeen.

Käyttäjänhallintalohko 24 ja istunnonohjauslohko 22 ovat edelleen yhteydessä järjestelmätiedostolohkoon tai tietokantaan 26, johon on muun muassa tallennettu käyttäjätiedot salasanoineen. Tietojen salaukseen liittyvä mahdollinen salausavainlista 8 sijaitsee esimerkiksi tietokannassa. Salausavainlista käsittää yhden tai useamman salausavaimen. Edelleen tietokannassa voi olla tieto siitä, miten salausavainlistaan kuuluvia salausavaimia muodostetaan. Istunnonohjauslohkon tehtävänä on muun muassa luoda indeksejä, jotka osoittavat salausavainlistan salausavaimiin. Indeksit muodostetaan esimerkiksi satunnaisesti tai tietyn algoritmin perusteella. Istunnonohjauslohko on lisäksi yhteydessä turvapalvelulohkoon 25. Turvapalvelulohko sisältää salaukseen tarvittavat salausalgoritmit ja suorittaa tietojen salauksen pyydettäessä. Eräs tällainen salausalgoritmi voi olla MD5. Tietojen salaukseen liittyvä mahdollinen salausavainlista voi vaihtoehtoisesti sijaita turvapalvelulohkossa.

Turvapalvelulohko 25 käsittää ohjelmalohkon 1, jolla muodostetaan salausavaimia. Ohjelmalohko 1 tarkoittaa esimerkiksi lohkoa, joka sisältää salausalgoritmin. Ohjelmalohko 1 voi käsittää tietyn ennalta määrätyn algoritmin, joka tuottaa kyseisiä salausavaimia. Turvapalvelulohko käsittää ohjelmalohkon 2, jolla salataan salattavaksi tarkoitettuja tietoja. On mahdollista, että ohjelmalohkot 1 ja 2 yhdessä muodostavat isomman ohjelmalohkon.

Käyttäjänhallintalohko 24 käsittää ohjelmalohkon 4, joka suorittaa vertailuja. Vertailtavina osapuolina ovat esimerkiksi salatut käyttäjätunnukseen liittyvät salasanat. Käyttäjänhallintalohko käsittää

edelleen ohjelmalohkon 5, jolla hyväksytään muodostettava etäistunto. Lisäksi käyttäjänhallintalohko käsittää ohjelmalohkon 6, jolla estetään etäistunnon muodostaminen. Etäistunnon muodostaminen estetään esimerkiksi silloin, kun ohjelmalohko 4 tuottaa negatiivisen tuloksen vertailutoimenpiteessä. Ohjelmalohkot 5 ja 6 voivat yhdessä muodostaa isomman ohjelmalohkon.

Ohjelmalohkolla 27 tarkoitetaan esimerkiksi ohjelmalohkoa PB tai käytönohjauslohkoa MMSSEB, joka sijaitsee toisessa järjestelmässä.

Kuvassa 3 esitetään eräs edullinen vuokaavioesimerkki keksinnön mukaisesta toiminnasta. Lohkon 30 mukaisesti valitaan tai muodostetaan indeksi. Indeksi voi olla satunnaisluku tietyltä väliltä tai sitten se voidaan muodostaa esimerkiksi salaisella algoritmilla. Muodostettavalla indeksillä on vaatimuksena, että se osoittaa johonkin lähde- ja kohdejärjestelmässä olevaan salausavaimeen. Salausavain sijaitsee esimerkiksi erityisessä salausavainlistassa. Käyttäjätunnukset ja niihin liittyvät salasanat on tallennettu sekä lähde- että kohdejärjestelmään. Lisäksi tässä esimerkissä molempiin järjestelmiin on tallennettu identtinen salausavainlista. On huomattava, että salausavainlistaa ei ole välttämätöntä muodostaa vaan salausavaimet voidaan muodostaa myös muilla tavoin. Lohkon 31 mukaisesti käyttäjätunnukseen liittyvä salasana salataan juuri tuotetun ensimmäisen indeksin osoittamalla salausavainlistan salausavaimella. Käytettävä salausalgoritmi on edullisesti ns. yksisuuntainen algoritmi. Eräs tällainen algoritmi on MD5. Yksisuuntainen algoritmi tarkoittaa sitä, että salauksen lopputuloksesta ei ole mahdollista päätellä tai muodostaa alkuperäistä syötettä.

Jotta järjestelmät voisivat varmistua toisistaan, tunnistusta varten muodostetaan erillinen tunnistetieto ja salataan se samaisen ensimmäisen indeksin osoittamalla salausavaimella, lohko 32. Tunniste-

tieto tarkoittaa esimerkiksi aikatietoa, joka saadaan järjestelmän kellosta. Olennaista on, että tunnistetieto on luonteeltaan muuttuvaa. Tunnistetiedon käyttö ei ole pakollista, mutta tässä esimerkissä sitä käytetään. Tässä esimerkissä tunnistetieto lähetetään yhdessä käyttäjätietojen kanssa. On myös mahdollista, että tunnistetieto lähetetään erillään käyttäjätiedoista muuna sopivana ajankohtana. Lohkon 33 mukaisesti indeksi ja salattu tunnistetieto tallennetaan lähdejärjestelmään myöhempää käyttöä varten. Lähdejärjestelmä lähettää käyttäjätunnuksen, ensimmäisen indeksin, salatun tunnistetiedon ja salasanan kohdejärjestelmälle, lohko 34. Koska tässä esimerkissä salasana on alunperinkin tallennettuna salatussa muodossa lähde- ja kohdejärjestelmässä, tässä esimerkin vaiheessa se on salattu kaksinkertaisesti eri avaimilla. Indeksi ja käyttäjätunnus voidaan lähettää salaamattomina siksi, ettei niiden julkisuus vähennä järjestelmän turvallisuutta, koska indeksiä vastaava salausavainlistan salausavain on suojatussa tiedostossa puhelinkeskuksessa.

Kohdejärjestelmä vastaanottaa lähetetyt tiedot ja etsii käyttäjätunnusta vastaavan salasanan omista tiedostoistaan, lohko 35. Tässä vaiheessa ei siis käsitellä vastaanotettua salasanaa. Kohdejärjestelmä salaa etsityn salasanan vastaanotetun viestin määrittelemän ensimmäisen indeksin mukaisella salausavaimella, lohko 36. Kuten aikaisemmin todettiin sekä lähde- että kohdejärjestelmä voivat sisältää identtiset salausavainlistat. On myös mahdollista, että lähde- ja kohdejärjestelmässä ei ole lainkaan varsinaisia salausavainlistoja. Tällöin sekä lähde- että kohdejärjestelmä sisältävät identtiset keinot muodostaa salausavaimia. Identtisellä keinolla tarkoitetaan tässä esimerkissä esimerkiksi sitä, että lähde- ja kohdejärjestelmä sisältävät saman algoritmin, jolla voidaan muodostaa salausavaimia.

Tämän jälkeen verrataan lähdejärjestelmältä saatua ja juuri muodostettua salasanaa keskenään, lohko 37, ja jos salasanat täsmäävät, edetään lohkoon 38. Lohkossa 38 valitaan tai muuten muodostetaan uusi, toinen indeksi. Lähdejärjestelmältä saatu kaksinkertaisesti salattu salasana salataan kolmannen kerran toisen indeksin osoittamalla salausavaimella, lohko 39. Samalla salataan vastaanotettu jo ennestään kerran salattu tunnistetieto uudelleen toisen indeksin osoittamalla salausavaimella. Tämän jälkeen kohdejärjestelmä lähettää toisen indeksin, kaksi kertaa salatun tunnistetiedon ja kolme kertaa salatun salasanan takaisin lähdejärjestelmälle, lohko 40.

Lähdejärjestelmä vastaanottaa kohdejärjestelmän lähettämät tiedot, jonka jälkeen se salaa alussa kohdejärjestelmälle lähetetyn salasanan ja tunnistetiedon toisen indeksin osoittamalla salausavaimella. Tällöin salasana on siis salattu jo kolme kertaa, lohko 41. Toista indeksiä vastaava salasana löytyy esimerkiksi salausavainlistasta. Saatua kolminkertaisesti salattua salasanaa verrataan kohdejärjestelmältä saatuun myöskin kolminkertaisesti salattuun salasaan, lohko 42. Jos salasanat ovat yhtenevät, käyttäjä on varmuudella tunnistettu.

Lohkon 43 mukaisesti lähdejärjestelmässä salataan alussa ensimmäisen indeksin osoittamalla salausavainlistan salausavaimella salattu tunnistetieto uudelleen vastaanotetun toisen indeksin osoittamalla salausavainlistan salausavaimella. Tämän jälkeen verrataan tulosta kohdejärjestelmältä vastaanotettuun kaksinkertaisesti salattuun tunnistetietoon, lohko 44. Jos salatut tunnistetiedot eivät poikkea toisistaan, kohdejärjestelmä on varmuudella se, jonka se pitikin olla.

Edellä kuvatut tunnistetiedon välitys- ja salaustoimenpiteet varmistavat sen, että kukaan ulkopuolinen käyttäjä ei ole kaapannut ensimmäistä lähdejär-

jestelmän kohdejärjestelmälle lähettämää sanomaa. Täten tunnistetiedon käyttö estää sen, että ulkopuolinen taho kykenisi valheellisesti esittämään kohdejärjestelmää lähdejärjestelmälle.

Keksintöä ei rajata pelkästään edellä esitettyjä sovellusesimerkkejä koskevaksi, vaan monet muunnokset ovat mahdollisia pysyttäessä patenttivaatimusten määrittelemän keksinnöllisen ajatuksen puitteissa.

PATENTTIVAATIMUKSET

1. Menetelmä käyttäjän tunnistamiseksi ja osapuolten varmistamiseksi tietoliikennejärjestelmässä, joka käsittää:

tietoliikenneverkon (OM);

lähdejärjestelmän (LE1), joka on yhdistetty tietoliikenneverkkoon (OM);

kohdejärjestelmän (LE2), joka on yhdistetty tietoliikenneverkkoon (OM);

joka menetelmä käsittää vaiheet:

tallennetaan lähdejärjestelmään (LE1) ja kohdejärjestelmään (LE2) käyttäjätunnukset ja niihin liittyvät salasanat;

kirjaudutaan lähdejärjestelmään (LE1) syöttämällä käyttäjätunnus ja sitä vastaava salasana;

tunnistetaan käyttäjä lähdejärjestelmässä (LE1);

muodostetaan etäistunto kohdejärjestelmään (LE2);

t u n n e t t u siitä, että menetelmä edelleen käsittää vaiheet:

muodostetaan lähdejärjestelmään (LE1) ja kohdejärjestelmään (LE2) identtiset indeksoidut salausavaimet;

salataan käyttäjätunnukseen liittyvä salasana lähdejärjestelmässä (LE1) ensimmäisen indeksin osoittamalla salausavaimella ja lähetetään salatut tiedot sekä ensimmäinen indeksi ja käyttäjätunnus kohdejärjestelmälle (LE2);

salataan käyttäjätunnukseen liittyvä salasana kohdejärjestelmässä (LE2) vastaanotetun indeksin osoittamalla salausavaimella;

tehdään ensimmäinen vertailu vastaanotetun salatun salasanan ja kohdejärjestelmässä (LE2) salatun salasanan välillä;

salataan kohdejärjestelmässä (LE2) lähdejärjestelmältä (LE1) vastaanotettu salattu salasana toisen indeksin osoittamalla salausavaimella ja lähetetään salatut tiedot sekä toinen indeksi lähdejärjestelmälle (LE1);

salataan alussa lähdejärjestelmältä (LE1) kohdejärjestelmälle (LE2) lähetetty salattu salasana uudestaan kohdejärjestelmältä (LE2) vastaanotetun toisen indeksin osoittamalla salausavaimella;

tehdään toinen vertailu kohdejärjestelmältä (LE2) vastaanotetun salatun salasanan ja lähdejärjestelmässä (LE1) ensimmäisen ja toisen indeksin osoittamilla salausavaimilla salatun salasanan välillä; ja

hyväksytään etäistunnon muodostus, jos vertailujen tulokset ovat yhteneväisiä.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että estetään etäistunnon muodostus, jos ensimmäisen tai toisen vertailun tulokset eivät ole yhtenevät.

3. Patenttivaatimuksen 1 tai 2 mukainen menetelmä, t u n n e t t u siitä, että

muodostetaan erillinen tunnistetieto;

salataan tunnistetieto lähdejärjestelmässä (LE1) ensimmäisen indeksin osoittamalla salausavaimella ja lähetetään salatut tiedot kohdejärjestelmälle (LE2);

salataan kohdejärjestelmässä (LE2) lähdejärjestelmältä (LE1) vastaanotettu tunnistetieto toisen indeksin osoittamalla salausavaimella ja lähetetään salatut tiedot sekä toinen indeksi takaisin lähdejärjestelmälle (LE1);

salataan lähdejärjestelmässä (LE1) alussa kohdejärjestelmälle (LE2) lähetetty ensimmäisen indeksin osoittamalla salausavaimella salattu tunnistetieto uudestaan kohdejärjestelmältä (LE2) vastaanotetun toisen indeksin osoittamalla salausavaimella;

tehdään kolmas vertailu kohdejärjestelmältä (LE2) vastaanotetun salatun tunnistetiedon ja lähdejärjestelmässä (LE1) juuri salatun tunnistetiedon välillä; ja

hyväksytään etäistunnon muodostus, jos vertailun tulos on yhteneväinen.

4. Patenttivaatimuksen 3 mukainen menetelmä, t u n n e t t u siitä, että estetään etäistunnon muodostus, jos kolmannen vertailun tulos ei ole yhteneväinen.

5. Jonkin edeltävistä patenttivaatimuksista 1 - 4 mukainen menetelmä, t u n n e t t u siitä, että

lähetetään tunnistetieto samanaikaisesti käyttäjätietojen kanssa; tai

lähetetään tunnistetieto erillään käyttäjätiedoista.

6. Jonkin edeltävistä patenttivaatimuksen 1 - 5 mukainen menetelmä, t u n n e t t u siitä, että liitetään tunnistetietoon aikatieto ja/tai lähdejärjestelmän yksilöivä tieto.

7. Jonkin edeltävistä patenttivaatimuksista 1 - 6 mukainen menetelmä, t u n n e t t u siitä, että muodostetaan salausavaimet tietyllä ennalta määritellyllä algoritmilla.

8. Jonkin edeltävistä patenttivaatimuksista 1 - 7 mukainen menetelmä, t u n n e t t u siitä, että tallennetaan salausavaimet erityiseen salausavainlistaan.

9. Jonkin edeltävistä patenttivaatimuksista 1 - 8 mukainen menetelmä, t u n n e t t u siitä, että muodostetaan indeksi satunnaisesti tai jonkin ennalta määritellyn algoritmin pohjalta.

10. Jonkin edeltävistä patenttivaatimuksista 1 - 9 mukainen menetelmä, t u n n e t t u siitä, että käytetään lähdejärjestelmässä (LE1) ja kohdejärjestelmässä (LE2) tiedon salaukseen yksisuuntaista salausalgoritmia.

11. Jonkin edeltävistä patenttivaatimuksista 1 - 10 mukainen menetelmä, t u n n e t t u siitä, että tietoliikennejärjestelmä on puhelinkeskusjärjestelmä.

12. Jonkin edeltävistä patenttivaatimuksista 1 - 11 mukainen menetelmä, t u n n e t t u siitä, että lähdejärjestelmä (LE1) ja/tai kohdejärjestelmä (LE2) ovat puhelinkeskuksia.

13. Jonkin edeltävistä patenttivaatimuksista 1 - 12 mukainen menetelmä, t u n n e t t u siitä, että tietoliikenneverkko (OM) on käytönohjausverkko.

14. Järjestelmä käyttäjän tunnistamiseksi ja osapuolten varmistamiseksi tietoliikennejärjestelmässä, joka käsittää:

tietoliikenneverkon (OM);

lähdejärjestelmän (LE1), joka on yhdistetty tietoliikenneverkkoon (OM);

kohdejärjestelmän (LE2), joka on yhdistetty tietoliikenneverkkoon (OM);

jossa järjestelmässä on mahdollista tallentaa lähdejärjestelmään (LE1) ja kohdejärjestelmään (LE2) käyttäjätunnukset ja niihin liittyvät salasanat, kirjautua lähdejärjestelmään (LE1) syöttämällä käyttäjätunnus ja sitä vastaava salasana, tunnistaa käyttäjä lähdejärjestelmässä (LE1) ja muodostaa etäistunto kohdejärjestelmään (LE2);

t u n n e t t u siitä, että järjestelmä käsittää:

välineet (1) identtisten indeksoitujen salausavainten muodostamiseksi lähdejärjestelmään (LE1) ja kohdejärjestelmään (LE2);

välineet (2) tietojen salaamiseksi lähde- ja kohdejärjestelmässä indeksin osoittamalla salausavaimella;

välineet (3) tietojen lähettämiseksi lähde- ja kohdejärjestelmän välillä;

välineet (4) vertailun tekemiseksi lähde- ja kohdejärjestelmässä; ja

välineet (5) etäistunnon muodostuksen hyväksymiseksi.

15. Patenttivaatimuksen 14 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmä käsittää välineet (6) etäistunnon muodostamisen estämiseksi.

16. Patenttivaatimuksen 14 tai 15 mukainen järjestelmä, t u n n e t t u siitä, järjestelmä käsittää

välineet (7) tunnistetiedon muodostamiseksi ja aikatiedon ja/tai lähdejärjestelmän yksilöivän tiedon liittämiseksi tunnistetietoon.

17. Jonkin edeltävistä patenttivaatimuksista 14 - 16 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmä käsittää salausavainlistan (8) salausavainten tallentamista varten.

18. Jonkin edeltävistä patenttivaatimuksista 14 - 17 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmä käsittää välineet (9) indeksin muodostamiseksi satunnaisesti tai jonkin ennalta määritellyn algoritmin pohjalta.

19. Jonkin edeltävistä patenttivaatimuksista 14 - 18 mukainen järjestelmä, t u n n e t t u siitä, että tietoliikennejärjestelmä on puhelinkeskusjärjestelmä.

20. Jonkin edeltävistä patenttivaatimuksista 14 - 19 mukainen järjestelmä, t u n n e t t u siitä, että lähdejärjestelmä (LE1) ja/tai kohdejärjestelmä (LE2) ovat puhelinkeskuksia.

21. Jonkin edeltävistä patenttivaatimuksista 14 - 20 mukainen järjestelmä, t u n n e t t u siitä, että tietoliikenneverkko (OM) on käytönohjausverkko.

(57) **TIIVISTELMÄ**

Menetelmä käyttäjän tunnistamiseksi ja osapuolten varmistamiseksi puhelinkeskusjärjestelmässä, joka käsittää tietoliikenneverkon (OM); lähdejärjestelmän (LE1), joka on yhdistetty tietoliikenneverkkoon (OM); ja kohdejärjestelmän (LE2), joka on yhdistetty tietoliikenneverkkoon (OM). Menetelmän mukaisesti tallennetaan lähdejärjestelmään (LE1) ja kohdejärjestelmään (LE2) käyttäjätunnukset ja niihin liittyvät salasanat; kirjaudutaan lähdejärjestelmään (LE1) syöttämällä käyttäjätunnus ja sitä vastaava salasana; tunnistetaan käyttäjä lähdejärjestelmässä (LE1); ja muodostetaan etäistunto kohdejärjestelmään (LE2). Keksinnössä muodostetaan lähdejärjestelmään (LE1) ja kohdejärjestelmään (LE2) identtiset indeksoidut salausavaimet ja salataan lähdejärjestelmän (LE1) ja kohdejärjestelmän (LE2) välinen kohdetietoliikenne tietyn indeksin osoittamalla salausavaimella ja suoritetaan eräänlainen kättelyoperaatio. Kättelyoperaation ansiosta käyttäjä voidaan tunnistaa varmuudella. Erillisen tunnistetiedon käytön ansiosta lähdejärjestelmä (LE1) ja kohdejärjestelmä (LE2) voivat varmistua toistensa alkuperästä.

(FIG. 1)

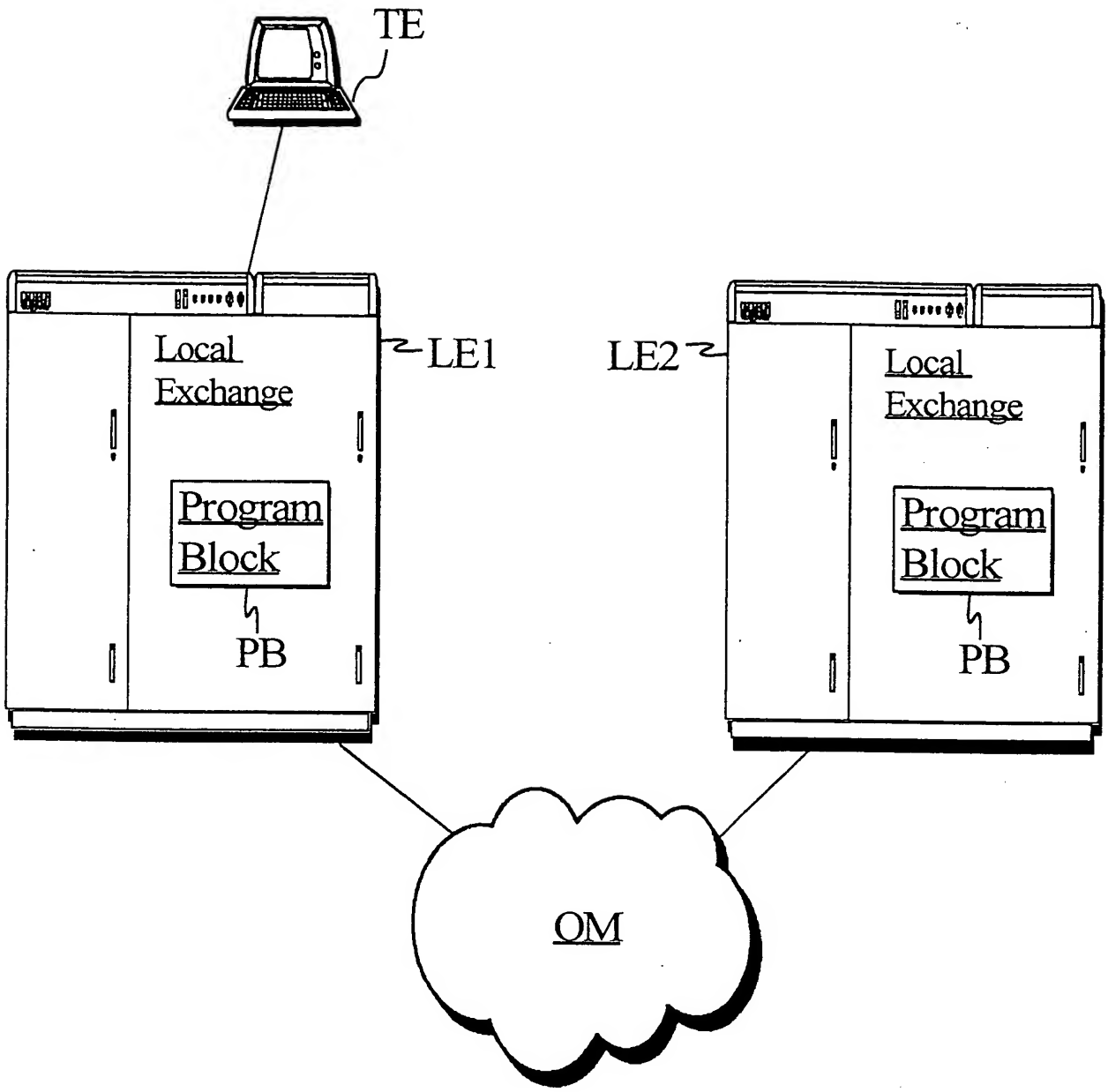
TE
Local
Exchange
LE1
Program
Block
PB
LE2
Local
Exchange
Program
Block
PB
OM

Fig. 1

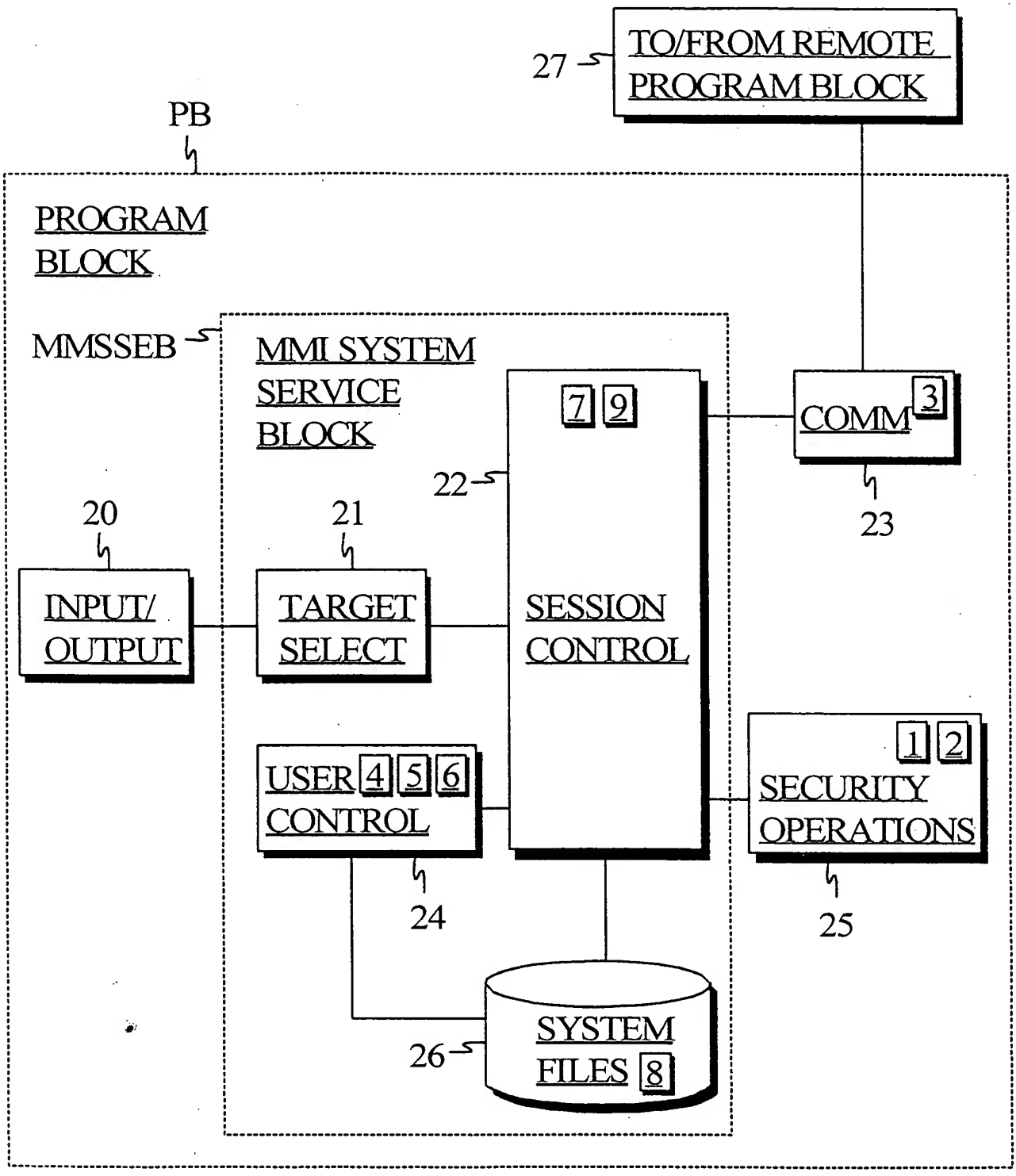
27
TO/FROM REMOTE PROGRAM BLOCK
PB
PROGRAM BLOCK
MMSSEB
MMI SYSTEM SERVICE BLOCK
7 9
COMM 3
22
23
20
21
INPUT/ OUTPUT
TARGET SELECT
SESSION CONTROL
USER 4 5 6 CONTROL
1 2
SECURITY OPERATIONS
24
25
SYSTEM FILES 8
26

Fig. 2

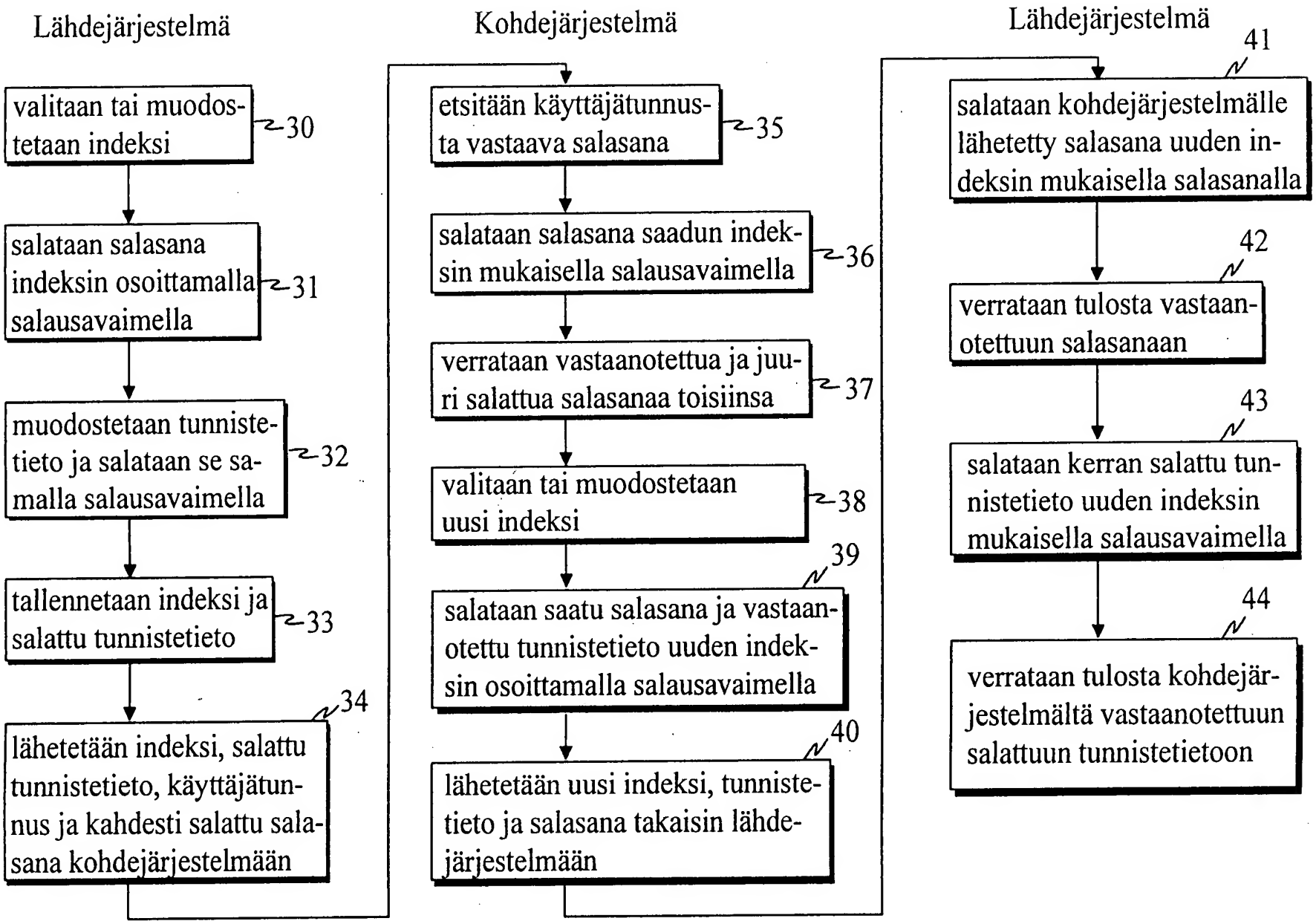
Lähdejärjestelmä
valitaan tai muodostetaan indeksi
30
salataan salasana indeksin osoittamalla salausavaimella
31
muodostetaan tunnistetieto ja salataan se samalla salausavaimella
32
tallennetaan indeksi ja salattu tunnistetieto
33
34
lähetetään indeksi, salattu tunnistetieto, käyttäjätunnus ja kahdesti salattu salasana kohdejärjestelmään
Kohdejärjestelmä
etsitään käyttäjätunnusta vastaava salasana
35
salataan salasana saadun indeksin mukaisella salausavaimella
36
verrataan vastaanotettua ja juuri salattua salasanaa toisiinsa
37
valitaan tai muodostetaan uusi indeksi
38
39
salataan saatu salasana ja vastaanotettu tunnistetieto uuden indeksin osoittamalla salausavaimella
40
lähetetään uusi indeksi, tunnistetieto ja salasana takaisin lähdejärjestelmään
Lähdejärjestelmä
41
salataan kohdejärjestelmälle lähetetty salasana uuden indeksin mukaisella salasanalla
42
verrataan tulosta vastaanotettuun salasanaan
43
salataan kerran salattu tunnistetieto uuden indeksin mukaisella salausavaimella
44
verrataan tulosta kohdejärjestelmältä vastaanotettuun salattuun tunnistetietoon

Fig. 3